v1.5 | 21 10 2020

Livre blanc de la sécurité HelloID

RENFORCER LA SECURITÉ ET LA CONFORMITÉ GRACE A L'AUTHENTIFICATION UNIQUE ET AU MFA

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

INDEX

Introduction

HelloID est une solution de gestion des identités et des accès (IAM) basée sur le cloud qui fournit un service d'authentification unique. L'authentification unique (SSO) garantit à vos utilisateurs l'accès à toutes leurs applications et données d'entreprise via un portail unique, ne nécessitant qu'un seul nom d'utilisateur et mot de passe. En outre, HelloID contient également des modules d'automatisation des actions dans le SI (Service Automation) ainsi que de provisionning/gestion des comptes utilisateurs.

Grâce à sa fonctionnalité d'authentification unique, HelloID prend en charge toutes les applications d'entreprise qu'elles soient dans le cloud ou sur site. La mise en place de cette simplification des accès peut être rendue plus sécurisée par l'implémentation (option gratuite intégrée dans HelloID) de l'authentification à deux facteurs et via de nombreuses politiques d'accès facilement configurables.

La sécurité est le thème central lors du déploiement de l'authentification unique (SSO) :

- **Le SSO intégre de manière transparente un système de protection lors du processus de connection** afin d'allier utilisation intuitive, sécurité et conformité. Réduire les informations d'identification à un seul nom d'utilisateur et mot de passe simplifie l'accès, favorise une culture de sécurité plus disciplinée (complexité du mot de passe, changement régulier, etc.) et prend en charge la conformité aux nouvelles lois sur les données et la confidentialité.
- **La solution SSO offre une plus grande sécurité grâce à son « point d'accès unique » protégé**. Cela signifie que la sécurité de la solution doit être un élément clé tout au long de son étude, de sa mise en œuvre et de son déploiement.

Ce livre blanc examine ces sujets de sécurité au sein de la solution IDaaS HelloID basée dans le cloud. Vous pouvez lire ce document conjointement aux deux autres livres blancs Tools4ever :

- Le *Livre Blanc HelloID*, qui fournit une introduction à toutes les fonctionnalités, caractéristiques et avantages de HelloID.
- Le *Livre Blanc Tools4ever des principes du Cloud*, qui explique notre vision globale de l'utilisation de la technologie cloud pour les solutions de gestion des identités et des accès.

Dans ce livre blanc, nous nous concentrons sur les principes de sécurité tels que ceux pris en charge et implémentés dans la solution HelloID. Nous abordons ici les sujets suivants :

- Comment la solution HelloID améliore la sécurité et aide les entreprises à se conformer davantage aux réglementations en matière de protection des données et de confidentialité.
- Les choix architecturaux et conceptuels faits pour assurer la sécurité dans l'ensemble de la solution HelloID, y compris les fonctions d'automatisation, de provisionning et de gouvernance des accès.
- Comment HelloID est testée par une entitée indépendante selon des exigences de sécurité claires, des normes pertinentes et comment cela est vérifié et certifié.

1. VUE D'ENSEMBLE DE LA SOLUTION HELLOID

Avec plus de 20 ans d'expérience dans les solutions de gestion des identités et plus de 10 millions d'utilisateurs actifs aux États-Unis, aux Pays-Bas, au Royaume-Uni, en Allemagne et en France, Tools4ever est un leader du marché de la gestion des identités et des accès. Nous servons un large éventail d'organisations dans tous les secteurs et de différentes tailles allant de 300 à plus de 200 000 comptes utilisateurs. HelloID, initialement développé en tant que plate-forme d'authentification unique dans le cloud, est l'une de nos solutions clés.

HelloID équipe les entreprises d'une solution IDaaS entièrement basée sur le cloud qui améliore leur environnement informatique. Cette plate-forme éditée par Tools4ever permet la transition d'une infrastructure sur site vers une infrastructure entièrement basée sur le cloud.

HelloID comprend trois composants :

1. Access Management : gère l'accès des utilisateurs aux différentes applications.
2. Service Automation : permet aux utilisateurs de faire des demandes en ligne à leur responsable et aux responsables d'appliquer automatiquement les modifications des paramètres dans le réseau, sans avoir à solliciter le HelpDesk.
3. Provisioning : connecte les systèmes sources tels que les ressources humaines, aux ressources du réseau pour permettre l'automatisation de la gestion des comptes utilisateurs lors de leurs arrivées, mobilités internes et départs.

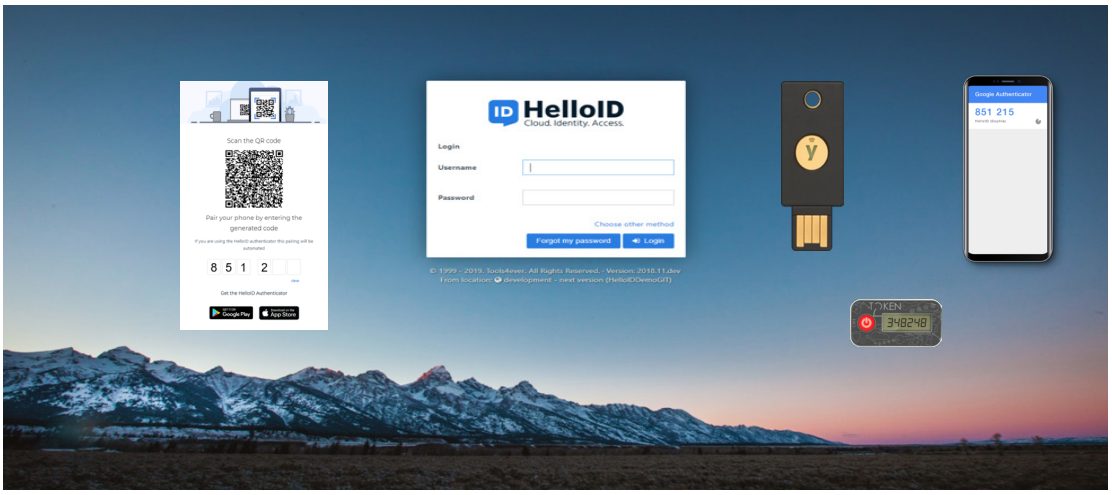
Les composants de HelloID fournissent aux organisations une base complète pour gérer en toute sécurité les identités des utilisateurs. Indépendamment de son environnement existant, de ses processus commerciaux ou d'autres structures, HelloID aide toute organisation à mettre en place une solution de gestion d'identité à part entière. Une implémentation rapide et des contrôles de gestion intuitifs facilitent l'adoption de HelloID. Maximiser la valeur et minimiser les délais de retour sur investissement sont les maîtres mots de cette solution.

La feuille de route à court terme de HelloID comprend des modules pour automatiser entièrement la gestion des rôles dans n'importe quelle organisation, telle que la gouvernance des accès. La fonctionnalité fournie par ces modules est déjà fournie par le portefeuille de produits de Tools4ever (IAM et UMRA), qui s'intègrent de manière transparente avec HelloID.

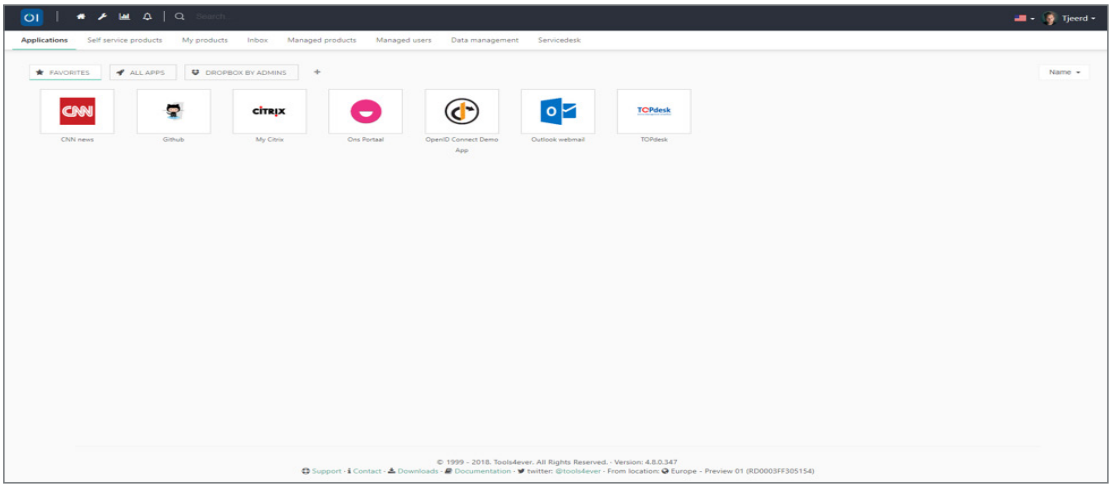
1.1. Gestion de l'accès unique via HelloID

Les utilisateurs finaux passent par trois étapes distinctes de la gestion des accès lorsqu'ils interagissent avec le processus de connexion de HelloID :

- L'Authentification: La première étape est l'authentification de l'utilisateur, qui s'effectue via une invite de connexion nécessitant un nom d'utilisateur et un mot de passe. Facultativement, une étape d'authentification à deux facteurs peut être ajoutée pour une vérification supplémentaire. Des informations contextuelles telles que l'heure, l'emplacement de connexion ou le type de navigateur peuvent également être utilisées pour vérifier l'accès.



- Le Tableau de bord : Après une authentification réussie, l'utilisateur a accès à un tableau de bord d'icônes d'application reconnaissables. Les icônes disponibles dépendent des ressources et des autorisations spécifiques à l'utilisateur, affichant uniquement celles pour lesquelles l'accès a été accordé. Chaque icône sert de lien vers son application respective, présentée dans une disposition simple et visuellement attrayante dans le portail ou un tableau de bord mobile.



- Le Single-On : Selon le protocole d'authentification de l'application, HelloID utilise le protocole SSO approprié pour identifier et authentifier automatiquement les utilisateurs finaux « en aval » dans cette application. HelloID prend en charge tous les protocoles SSO actuels (par exemple SAML, OpenID, OAuth). Pour les applications qui ne prennent en charge aucun protocole SSO, HelloID utilise une extension de navigateur qui permet en mode plugin, de garantir une expérience SSO cohérente pour l'utilisateur final. Le plugin sert de facto de solution de « gestion des mots de passe ». Les mots de passe sont stockés de manière centralisée dans HelloID.

Grâce à HelloID, l'utilisateur ne se connecte qu'une seule fois pour accéder à toutes les applications qui lui sont attribuées via un tableau de bord propre, depuis n'importe quel emplacement, sur n'importe quel appareil.

1.2. De l'authentification unique « on-premise » au SSO basée dans le cloud

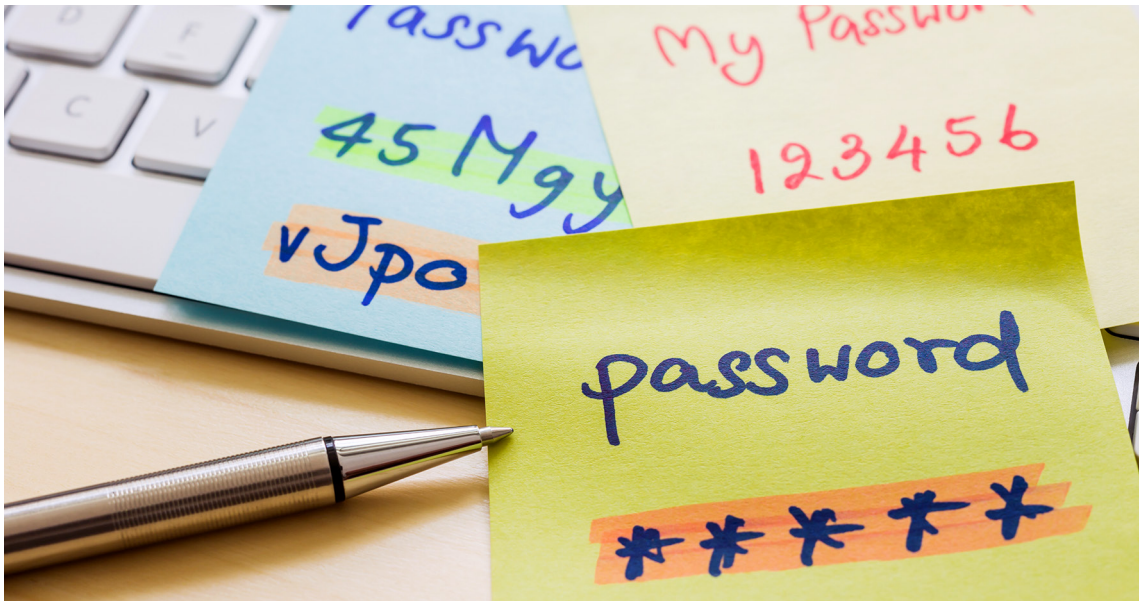
L'enquête Cloud RightScale 2019[1] a montré que 91% des entreprises utilisent déjà le cloud aujourd'hui, dont 94% utilisent une infrastructure de cloud public. En moyenne, les entreprises utilisent 4,8 offres cloud différentes dans toute la gamme des services privés, hybrides et publics.

Les clients de Tools4ever ont migré rapidement leurs paysages informatiques vers le cloud. Le principal moteur des migrations vers le cloud a été le besoin d'une plus grande flexibilité. De plus, les technologies cloud fournissent aux organisations une méthode rentable pour se concentrer principalement sur l'optimisation des opérations métier. Dans le cadre de ces stratégies de migration généralisées, nos clients exigent également que nos solutions de gestion des identités et des accès soient basées sur le cloud. Nous les avons écoutés.

Compte tenu de ces exigences et de notre ferme croyance dans la technologie cloud, nous avons commencé à mettre à niveau nos solutions de gouvernance et d'administration des identités pour passer d'une solution on-premise site vers le cloud. HelloID est notre première implémentation d'un produit « cloud-first ». Il est entièrement conçu, développé et testé pour le déploiement du cloud public. Il s'agit d'une étape importante pour Tools4ever et pour nos clients.

2. HELLOID SUPPORTE LA CONFIDENTIALITÉ, LA SÉCURITÉ ET LA CONFORMITÉ

Le Single Signe-on permet d'atténuer la « fatigue des mots de passe » et le chaos d'identité qui se produisent lorsque les utilisateurs doivent se souvenir d'un nombre excessif de mots de passe dans le cadre de leur activité quotidienne. Le SSO exige que les utilisateurs se souviennent d'un seul nom d'utilisateur et mot de passe, se connectant une seule fois pour accéder à toutes leurs applications. Ce résultat aide également grandement les administrateurs informatiques à consacrer plus de temps aux tâches importantes au lieu de gérer les appels au helpdesk liés aux mots de passe oubliés..



Malheureusement, ce scénario peut conduire certains à considérer à tort le but de l'authentification unique comme étant principalement axé sur la convivialité. Pire encore, la direction peut craindre qu'une unique paire Utilisateur/mot de passe présente un risque majeur. Cela présente à tort le SSO comme une simple passerelle entre les utilisateurs non autorisés et un accès complet et sans restriction aux applications et aux données de l'organisation..

Dans ce chapitre, nous développons la vision de Tools4ever de l'authentification unique comme un puissant coup de pouce intrinsèque à la gestion sécurisée des accès dans toute organisation. Par conséquent, le résultat assure une bien meilleure conformité aux lois sur la protection des données et à leurs confidentialité.

2.1. Le SSO favorise l'utilisation de mots de passe sécurisés

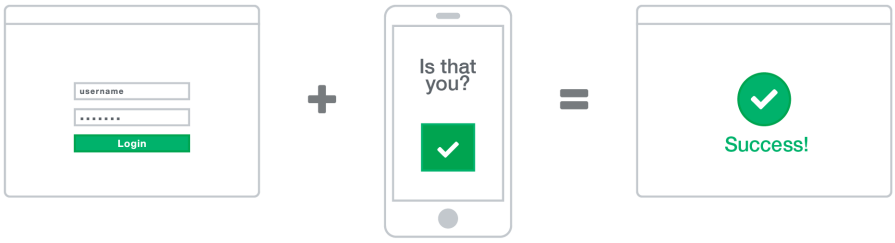
Si les utilisateurs doivent se souvenir de plusieurs noms d'utilisateur et mots de passe, ils commencent immédiatement à rechercher des solutions de contournement. Les systèmes deviennent peu sûrs avec des pratiques telles que l'écriture de mots de passe sur des post-it. Alternativement, les gens comptent sur des mots de passe simples et extrêmement vulnérables. En décembre 2019, « password », « 123456 » et « qwerty » figuraient toujours dans le top 10 des mots de passe les plus courants [2].

Pour atténuer ce problème, l'authentification unique permet aux employés d'éliminer leur vaste ensemble d'informations d'identification et de ne mémoriser qu'un seul nom d'utilisateur et mot de passe. Comme un seul mot de passe est utilisé beaucoup moins fréquemment, les mots de passe complexes et les « phrases secrètes » deviennent beaucoup moins problématiques. Cette approche aide également les organisations à appliquer plus facilement les politiques de changement de mot de passe et prend en charge l'intégration avec le logiciel de réinitialisation de mot de passe pour mieux faciliter les changements de mot de passe périodiques.

Par conséquent, l'authentification unique facilite souvent le passage de vastes collections de mots de passe très faibles à un mot de passe unique, solide, bien protégé et bien géré. Dans le scénario idéal, de fortes combinaisons nom d'utilisateur / mot de passe pour toutes les applications sont générées automatiquement dans le back-end par application. De cette façon, les utilisateurs finaux ne peuvent accéder aux applications que via le portail SSO.

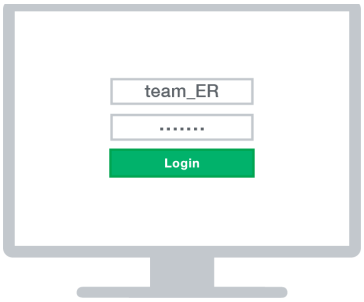
2.2. Le SSO prend en charge l'authentification forte

Le Single Sign-on permet aux entreprises de mettre en œuvre une authentification forte avec une « authentification à 2 facteurs » (2FA). Cela améliore la sécurité car les utilisateurs doivent saisir un deuxième code pour accéder au système ou à l'application, qui peut être fourni via un client dédié ou un SMS. Alors que 2FA offre une plus grande sécurité, les utilisateurs finaux chercheront toujours des solutions de contournement, à moins que la solution SSO n'élimine tout besoin supplémentaire d'informations d'identification supplémentaires après la connexion. HelloID prend en charge le 2FA par défaut et est configurable en fonction de l'utilisateur, de l'emplacement et/ou de l'heure.



2.3. Le SSO facilite l'introduction de comptes nominatifs

Pour des raisons de conformité, en particulier en ce qui concerne le RGPD, HIPAA, SOX et d'autres réglementations, les organisations doivent pouvoir tracer ce que chaque employé fait sur le réseau de l'entreprise et prouver que les personnes ne peuvent accéder qu'aux données pertinentes pour leur rôle. Dans de nombreuses organisations, les employés partagent des comptes génériques avec d'autres collègues, ce qui signifie qu'ils se connectent tous avec les mêmes informations d'identification pour accéder aux systèmes et aux applications.

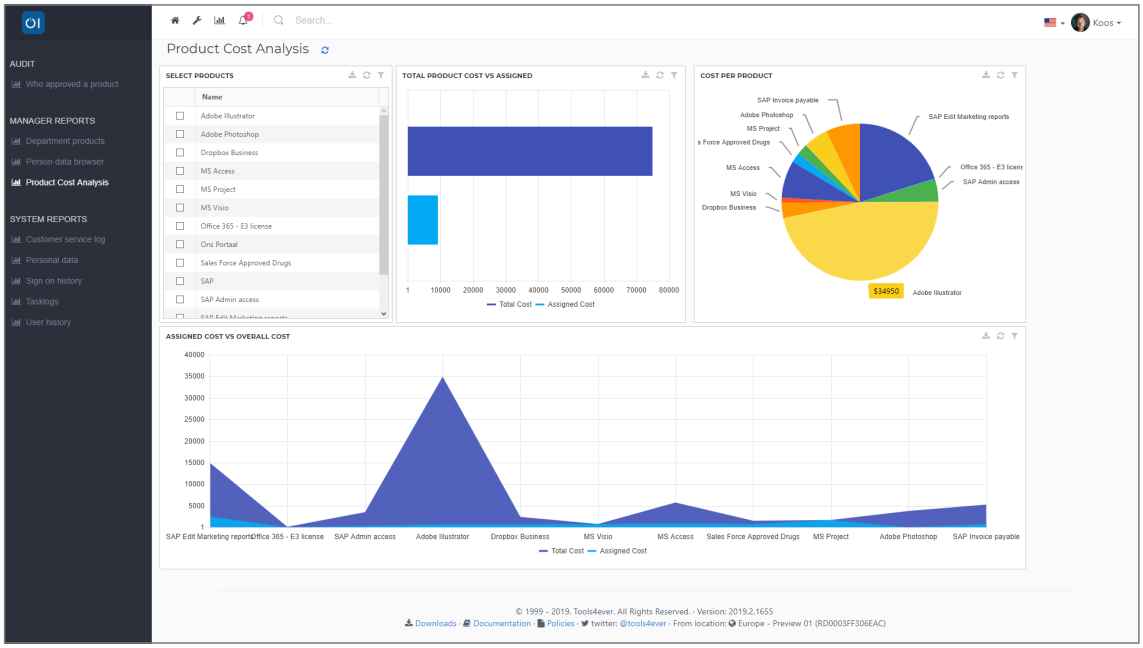


Comme il est impossible de déterminer quel employé a fait quoi pendant sa connexion, les organisations doivent éliminer les comptes partagés. Cependant, la suppression de ces comptes oblige les employés à se souvenir de plusieurs nouveaux ensembles d'informations d'identification pour chaque système ou application.

Une solution d'authentification unique résout ce problème et rationalise facilement le passage des comptes partagés aux comptes individuels et surveillés pour tout le monde. Avec une solution d'authentification unique, chaque employé devra se souvenir d'un seul ensemble d'informations d'identification dont la valeur lui est propre. Cela permet à l'organisation d'éliminer les comptes partagés et de se conformer aux lois sur la protection des données et la confidentialité sans trop perturber les procédures métier.

2.4. HelloID supporte facilement les rapports d'audit

La conformité aux réglementations nécessite un rapport d'audit complet sur tous les utilisateurs. Les solutions d'authentification unique doivent produire automatiquement des rapports d'audit via leur base de données centrale qui enregistre toutes les activités des utilisateurs ainsi qu'une copie cryptée de l'ensemble des informations d'identification de chaque utilisateur. Cette base de données doit également indiquer exactement quels comptes utilisateurs ont accès à quelles applications ainsi que les dates et heures d'accès. Les événements consignés incluent les connexions réussies et échouées, l'emplacement géographique de l'utilisateur, les appareils utilisés, les réinitialisations de mot de passe initiées, les tentatives d'accès aux applications et les échecs d'accès dus à la stratégie d'accès. Les journaux permettent aux organisations de stocker en toute sécurité ces informations aussi longtemps que la réglementation l'exige et de générer facilement des rapports d'audit chaque fois que cela est nécessaire, même des années après un événement donné.



3. LA SÉCURITÉ DE LA SOLUTION HELLOID

Comme décrit dans le chapitre précédent, la fonctionnalité SSO de HelloID favorise l'utilisation de mots de passe sécurisés et une authentification forte tout en facilitant l'utilisation de comptes nominatifs et en compilant des rapports d'audit. Étant donné que le « point d'accès unique » du SSO offre aux utilisateurs un accès complet à la gamme complète d'applications et de données affectées à leur rôle ou à leur fonction, la solution requiert une architecture intrinsèquement solide et bien entretenue. Dans ce chapitre, nous résumerons les principes fondamentaux que nous avons intégrés au cours du développement pour garantir une solution SSO sécurisée de manière optimale.

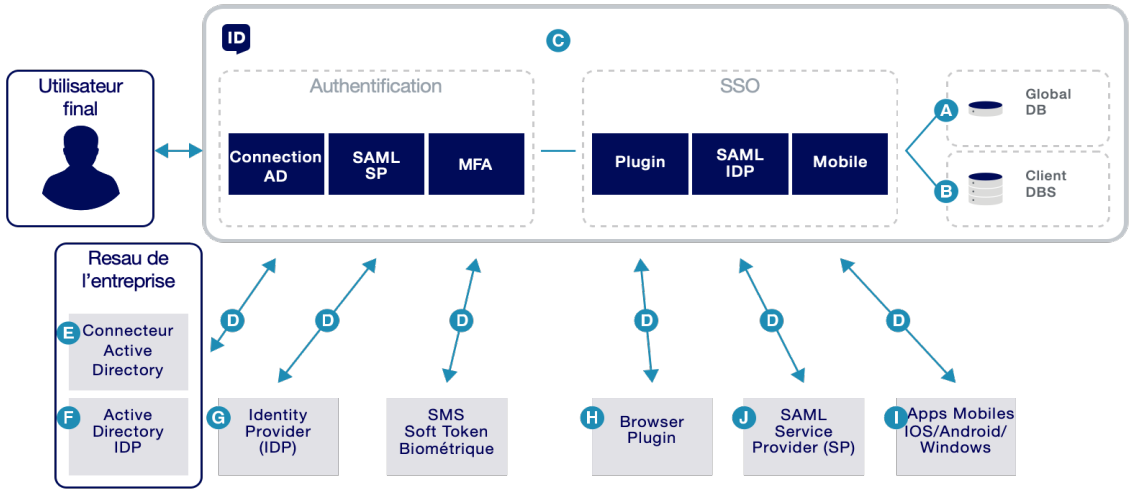
3.1. Les Principes de conception, du développement et de la sécurité

La façon dont nous concevons, développons et entretenons nos solutions est basée sur un ensemble de principes clés décrits ci-dessous. Les principes de sécurité dès la conception tels que définis par l'OWASP constituent le fondement de notre approche.

1	Minimiser la surface d'attaque	Notre objectif de développement sécurisé est de réduire le risque global en réduisant ce que l'on appelle la « surface d'attaque ». Chaque fonctionnalité ajoutée à une application ajoute un certain risque à l'application globale.
2	Valeurs hautes de sécurité par défaut	Par défaut, nous offrons une expérience utilisateur extrêmement sécurisée. Il appartient à l'utilisateur de l'application, dans le cadre de son mandat, de réduire selon les besoins le niveau de sécurité par défaut.
3	Principe du privilège minimal	Par défaut, les comptes disposent des privilèges minimaux requis pour effectuer les processus métier nécessaires. Cela couvre non seulement les droits des utilisateurs, mais également les autorisations de ressources telles que les limites du processeur, la mémoire, le réseau et les autorisations du système de fichiers.
4	Principe de défense à plusieurs niveaux	Même lorsqu'un seul contrôle serait raisonnable, nous préférons davantage de contrôles afin d'aborder les risques de différentes manières. Ce principe permet de réduire la probabilité d'exploitation de vulnérabilités graves.
5	Échec sécurisé	Une application peut ne pas traiter les transactions pour diverses raisons. Cependant, le résultat d'un tel échec détermine si une application est sécurisée ou non. Tous les composants HelloID sont conçus pour un « échec sécurisé ».
6	Ne pas faire confiance aux services par défaut	Les partenaires tiers auront généralement des politiques et procédures de sécurité différentes de la nôtre. Par conséquent, nous ne faisons pas implicitement confiance aux systèmes gérés en externe et traitons tous les systèmes externes de manière similaire.
7	Séparation des fonctions	Il s'agit d'un élément essentiel de la lutte contre la fraude dans les flux de processus des solutions mises en œuvre. Par exemple, les administrateurs ne doivent généralement pas être des utilisateurs de l'application.
8	Maintenir une sécurité simple	Notre approche privilégie un code simple et direct au lieu d'approches trop complexes. Aucun "double négatif" ou architecture complexe n'est utilisé, sauf en cas d'absolue nécessité.
9	Corriger correctement les problèmes de sécurité	Une fois qu'un problème de sécurité a été identifié, il est important de développer un test pour celui-ci et de comprendre la cause profonde du problème. Lorsque des modèles de conception sont utilisés, il est probable que le problème de sécurité soit répandu parmi toutes les bases de code, il est donc essentiel de développer le correctif approprié sans introduire de régressions.

3.2. La Plateforme de la solution HelloID

L'architecture HelloID se compose de plusieurs composants. Le diagramme ci-dessous donne un aperçu des composants les plus importants et de leur interaction. Que les informations soient en transit ou stockées (temporairement), les informations sont toujours cryptées. Le diagramme montre quels mécanismes de sécurité sont appliqués par niveau. Le degré de sécurité diffère selon le niveau et dépend de l'étendue de l'impact, du risque et de l'applicabilité technique.



HelloID est hébergé sur le cloud Microsoft Azure

HelloID est hébergé sur la plateforme de cloud computing Azure de Microsoft. Notre partenaire cloud Microsoft Azure est reconnu internationalement comme un leader mondial du marché de l'infrastructure en tant que service (IaaS) et a déployé une infrastructure cloud qui couvre entièrement les demandes mondiales et locales. En tirant parti de leur topologie leader et bien structurée par zones géographiques, régions et zones de disponibilité, nous pouvons garantir à nos clients les plus hauts niveaux de résilience des données. Étant donné qu'Azure possède des centres de données dans le monde entier, il est possible de placer la base de données client dans la région souhaitée par le client. Tools4ever a un partenariat Microsoft Gold de longue date et a acquis une expérience de sécurité spécifique en travaillant avec la suite de produits Microsoft.

La sécurité est intégrée dans le Cloud Microsoft dès le départ, en commençant par le cycle de vie du développement de la sécurité. Ce processus de développement obligatoire intègre les exigences de sécurité dans chaque phase du processus de développement. Le cycle de vie du développement de la sécurité garantit que le cloud Microsoft est protégé au niveau des couches physique, réseau, hôte, application et données afin que leurs services en ligne soient résistants aux attaques. La surveillance proactive continue, les tests de pénétration et l'application de directives de sécurité et de processus opérationnels rigoureux augmentent encore le niveau de détection et de protection dans l'ensemble du Cloud Microsoft.

La Sécurité des bases de données dans HelloID

La base de données HelloID contient des paramètres de configuration globale et des informations client (A). Ces informations sont cryptées à l'aide d'une clé de cryptage RSA 1024 bits. La base de données clients (B) contient toutes les configurations spécifiques au client et les données utilisateurs. Toutes les données sensibles sont cryptées à l'aide d'une clé de cryptage RSA 1024 bits. Chaque client a sa propre base de données et clé de chiffrement distinctes.

Le client peut configurer exactement quelles données utilisateur sont disponibles pour être récupérées à partir d'autres systèmes sources et stockées dans la base de données HelloID. Les administrateurs utilisent le « mappeur d'attributs » HelloID pour configurer les attributs utilisateur du système source (Active Directory (AD) dans cet exemple) qui seront utilisés dans la base de données HelloID. Ainsi, si le prénom d'un utilisateur est stocké dans AD, le client peut choisir si cet attribut sera rendu disponible dans HelloID. Ce mappage configurable garantit que la base de données HelloID reste toujours entièrement conforme à la politique de confidentialité et de sécurité de l'organisation.

Les communications Internet

Le serveur Web HelloID communique avec les composants via Internet à l'aide de HTTPS (D). Le niveau de cryptage est TLS 1.2, AES avec cryptage 256 bits.

3.3. Les éléments d'authentification

L'authentification d'un utilisateur final est la première étape d'un processus de connexion sécurisée pouvant être facilitée en suivant les éléments décrits dans cette section.

Authentification Active Directory

HelloID peut utiliser diverses sources pour authentifier les utilisateurs, comme par exemple l'Active Directory. Le connecteur Active Directory (E) installé sur le réseau de l'organisation facilite cette méthode. Le connecteur ne synchronise pas les informations d'identification avec le portail HelloID, il authentifie uniquement les utilisateurs par rapport à Active Directory lors de la connexion. Le connecteur Active Directory utilise HTTPS et s'authentifie auprès du portail à l'aide d'un « secret » partagé.

Le fournisseur d'identité Active Directory (F) est utilisé pour authentifier les utilisateurs à l'intérieur du réseau d'entreprise, permettant aux utilisateurs de se connecter sans fournir leurs informations d'identification (authentification Windows intégrée). Si l'utilisateur est connecté à Active Directory, il sera également automatiquement connecté à HelloID.

Authentification via un fournisseur d'identité externe

HelloID prend également en charge d'autres fournisseurs d'identité tels que OpenID Connect, Google, SalesForce, Azure, SAML et LDAP. Il est également possible d'utiliser la connexion du répertoire local de HelloID.

Par exemple, il est possible d'interagir avec un fournisseur d'identité externe compatible SAML pour authentifier les utilisateurs. Cette méthode ne nécessite aucune forme de synchronisation des informations d'identification. HelloID ne stocke pas les informations d'identification utilisées pour se connecter au fournisseur d'identité. L'authentification est purement basée sur les normes SAML et les redirections HelloID vers le portail IDP à des fins d'authentification et d'identification. L'administrateur système d'une organisation gère le certificat utilisé pour établir la connexion entre l'IDP et HelloID et stocke ce certificat dans la base de données de l'organisation. Merci de vous référer à « 4.1 SAML - Fournisseur d'identité (IDP) » pour une description détaillée d'une connexion SAML avec un IDP externe..

L'authentification à deux facteurs comme deuxième couche de vérification

Par la suite, une deuxième couche de vérification peut être requise pour authentifier l'utilisateur avant d'accorder l'accès. En plus des jetons logiciels ou durs et des SMS, différents mots de passe à usage unique (OTP) sont également pris en charge en tant qu'option 2FA. Selon les besoins de l'organisation, HelloID offre une variété d'options d'intégration, y compris l'intégration du client Radius.

Les politiques d'accès configurables

Les politiques d'accès régissent l'ensemble du processus de connexion, avec une configuration simple et intuitive fournie via le portail de gestion de HelloID. Il est possible de configurer des règles d'accès étendues en fonction, entre autres, du réseau, du type de réseau, de l'emplacement, de l'heure, du périphérique ou de l'application. L'administrateur HelloID de l'organisation détermine qui aura accès au portail ou à ses applications sous-jacentes et dans quelles conditions. Par exemple, il est possible de bloquer l'accès en fonction de différents critères :

- L'accès peut être refusé à partir de réseaux externes. Des restrictions géographiques peuvent être définies pour empêcher l'accès à partir de certains emplacements ou pays, y compris des plages d'adresses IP. Cette fonctionnalité augmente la sécurité des entreprises qui n'ont pas besoin d'accéder au portail depuis les pays spécifiés.
- Les restrictions horaires peuvent être configurées, c'est-à-dire que les groupes d'utilisateurs peuvent avoir un accès limité en fonction de l'heure, du jour de la semaine ou de dates spécifiques.
- L'accès peut être refusé en fonction de l'appareil (par exemple, tablettes ou smartphones) ou des navigateurs utilisés.

3.4. Le portail et les éléments d'authentification unique

Les utilisateurs sont redirigés vers leur portail personnel après la connexion, où ils peuvent ouvrir leurs applications en un seul clic et sans étapes de connexion supplémentaires. Les éléments suivants supportent ce processus.

La connexion aux applications

Pour activer l'authentification unique (SSO) pour les différentes applications, HelloID prend en charge tous les protocoles SSO existants tels que SAML, HTTP (S) Post, OpenID connect, Oauth, WS-Federation ou Basic Authentication. Même pour les applications anciennes ou si un fournisseur ne prend en charge aucun protocole SSO, HelloID fournit toujours un SSO via une extension de navigateur en mode « Plug-in ». Cela garantit un accès SSO vers toutes les applications.

Alors que le portail HelloID enregistre la connexion entre l'identité HelloID et les différentes applications, l'authentification auprès du portail et l'authentification auprès des différentes applications sont séparées pour des raisons de sécurité. Cela signifie que les jetons sont récupérés uniquement lors d'une demande d'accès plutôt que stockés, de sorte que les intrus malveillants ne peuvent pas y accéder facilement. L'utilisateur peut mettre fin à la session sans avoir à se reconnecter, fermant rapidement les applications et minimisant les risques d'une mauvaise utilisation. L'organisation contrôle entièrement qui peut accéder à quelles applications.

Le Plugin de navigateur et les applications mobiles

HelloID ne stocke pas les informations d'identification ni aucune autre information personnelle localement dans un plugin de navigateur (H). Pour chaque nouvelle session d'application, une demande est envoyée au portail HelloID pour vérifier si l'utilisateur est toujours connecté et pour demander les informations d'identification pour l'application choisie par l'utilisateur final.

HelloID a une application disponible pour chaque plate-forme mobile (par exemple, smartphones et tablettes) (I) afin d'interagir avec le portail HelloID pour l'authentification principale et à des fins d'authentification unique sur les sites Web mobiles. Les utilisateurs finaux doivent s'identifier une fois, dans un délai configurable. Le délai peut être réglé de 0 jour à permanent. La norme est tous les 30 jours. Les informations d'identification IDP sont stockées dans la mémoire d'exécution, jamais sur l'appareil. Pour la gestion des informations d'identification, HelloID utilise le même mécanisme que pour les plugins (voir (H), ci-dessus). Il n'y a pas de stockage local ni de mise en cache des informations d'identification de l'application.

3.5. La journalisation et les rapports

HelloID enregistre tous les événements importants. Ces événements incluent les connexions réussies et échouées, l'emplacement de l'utilisateur, les appareils utilisés, les réinitialisations de mot de passe lancées, les tentatives d'accès aux applications et les échecs d'accès dus à la stratégie d'accès. Ces événements peuvent être utilisés pour créer des rapports de sécurité détaillés. Ces rapports peuvent être utilisés pour identifier les menaces possibles et / ou fournir une piste d'audit. Des rapports peuvent être créés (entre autres) pour les scénarios suivants :

- Échecs de connexion multiples pour des comptes spécifiques.
- Tentative d'accès lorsque les stratégies d'accès s'appliquent.
- Échec de l'authentification à deux facteurs.
- Accès aux applications pour un compte spécifique.

Les informations enregistrées peuvent être récupérées à l'aide d'une API pour le traitement par des outils de Business Intelligence tels que PowerBI. HelloID fournit également un tableau de bord, qui présente des informations en temps réel sur ces événements. Sur la base de ces informations, des stratégies d'accès peuvent être configurées pour empêcher certains événements de se produire. Par exemple, si les informations révèlent qu'un utilisateur accède à une application spécifique à partir d'un appareil mobile, et cela est contraire à la politique de l'entreprise, un administrateur peut interdire une telle opération.

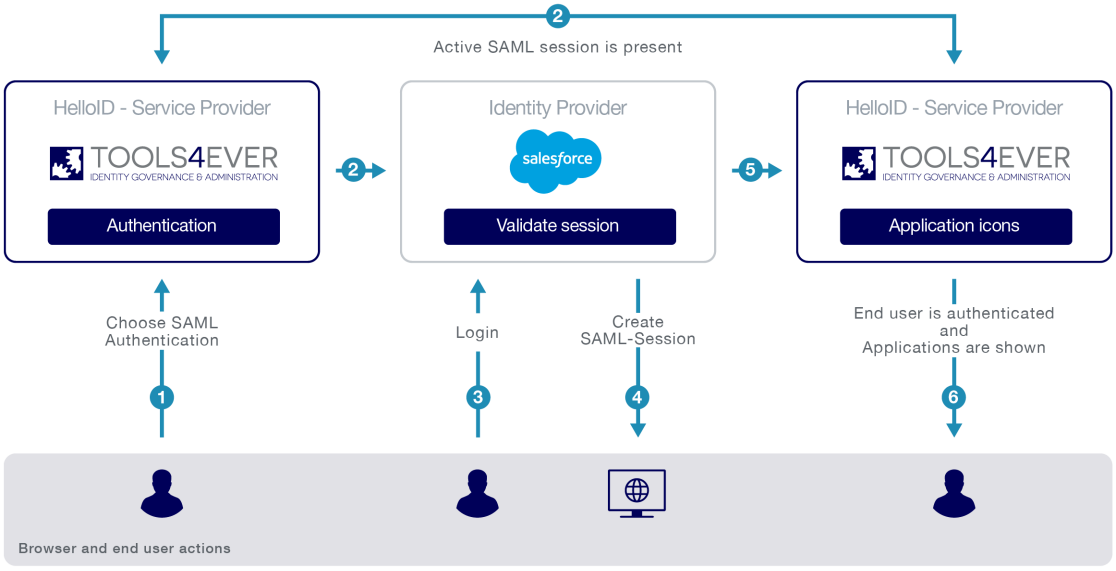
4. EXEMPLES DE SCÉNARIOS HELLOID

Le chapitre précédent décrit les différents composants de la solution HelloID. Ce chapitre décrit plus en détail certains scénarios d'authentification / SSO.

4.1. SAML - Fournisseur d'identité (IDP) vers HelloID (fournisseur de services)

Le SAML fournit les mécanismes permettant d'identifier un utilisateur final à l'aide d'un autre tiers de confiance (l'IDP). Les IDP courants sont Salesforce, Google et Amazon, mais d'autres tiers peuvent facilement servir d'IDP de confiance. HelloID peut être configuré pour faire confiance à n'importe quel IDP via le protocole SAML 2.0. Les certificats peuvent être échangés et définis par les administrateurs système dans le portail HelloID. Les informations du certificat sont stockées dans la base de données clients, comme illustré sur le diagramme ci-dessous.

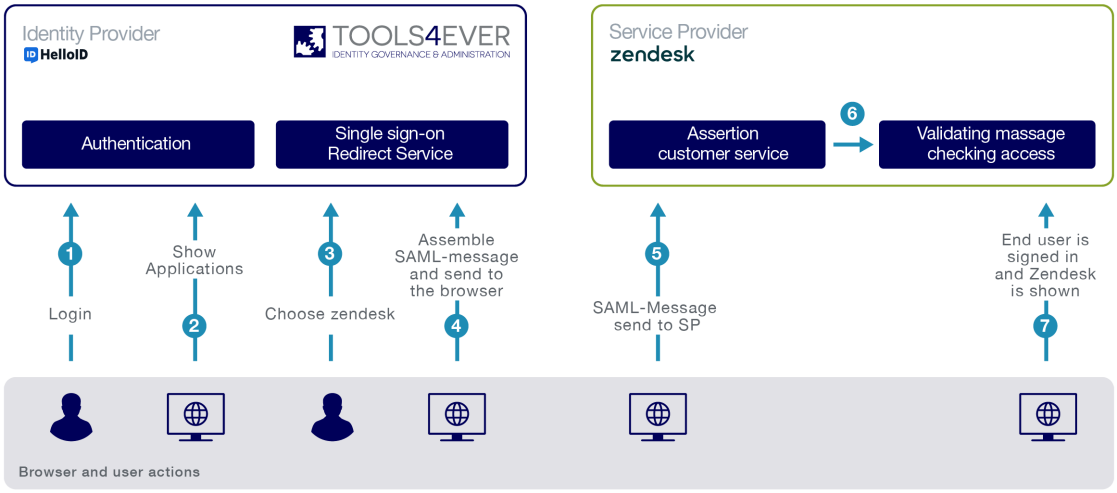
Étape 1	L'utilisateur accède au portail HelloID à l'aide de HTTPS. Chaque client recevra son propre domaine / URL unique. La première étape est l'authentification de l'utilisateur final. Plusieurs méthodes d'authentification sont disponibles pour la configuration. Le schéma ci-dessous explique la configuration IDP SAML.
Étape 2	Si aucune session SAML valide n'est détectée, l'utilisateur est redirigé vers le fournisseur d'identité et l'utilisateur est invité à s'identifier (étape 3). Si une session SAML valide est détectée, on passe à l'étape 5.
Étape 3	L'utilisateur se connecte au fournisseur d'identité. HelloID fait entièrement confiance à l'authentification fournie par cet IDP (telle que configurée dans HelloID).
Étape 4	Une fois l'identification réussie, une session SAML est créée par l'IDP et transmise à HelloID pour passer à l'étape 6.
Étape 5	Si une session valide est disponible, l'utilisateur final est redirigé vers le portail HelloID et toutes les applications auxquelles l'utilisateur peut accéder.
Étape 6	L'utilisateur est redirigé vers le portail HelloID et est connecté.



4.2. SAML - HelloID (en tant qu'IDP) vers le fournisseur de services (SP)

Le mécanisme d'authentification unique le plus courant et accepté pour les applications Web est le SAML 2.0. Le protocole est largement adapté et mis en œuvre par de nombreux éditeurs de logiciels. HelloID peut servir de partie IDP de confiance pour une application compatible SAML (appelée SP). En cas d'authentification réussie via le portail HelloID, cliquer sur n'importe quelle icône d'application sur le tableau de bord créera une session SAML avec le SP pour se connecter et accéder automatiquement à la ressource. Le diagramme ci-dessous décrit ce processus.

Étape 1	L'utilisateur accède au portail HelloID via HTTPS. Chaque client recevra son propre domaine / URL unique. La première étape est l'authentification de l'utilisateur final. La méthode d'authentification peut varier et n'est pas déterminée par le protocole SSO du portail. Par exemple, un utilisateur final peut utiliser le connecteur Active Directory pour l'authentification, puis utiliser SAML pour accéder aux applications via SSO.
Étape 2	HelloID affiche le tableau de bord de l'utilisateur contenant toutes les applications auxquelles l'utilisateur peut accéder.
Étape 3	L'utilisateur choisit le fournisseur de services (dans ce cas, Zendesk).
Étape 4	HelloID crée une session SAML avec ou dans le navigateur. Le SP détermine le type de session le plus efficace. Cela peut être une session mémoire du navigateur ou une session stockée dans un cookie.
Étape 5	Le navigateur est invité à se rediriger vers le fournisseur de services.
Étape 6	La signature du message SAML est validée par Zendesk.
Étape 7	L'utilisateur est automatiquement connecté à Zendesk.

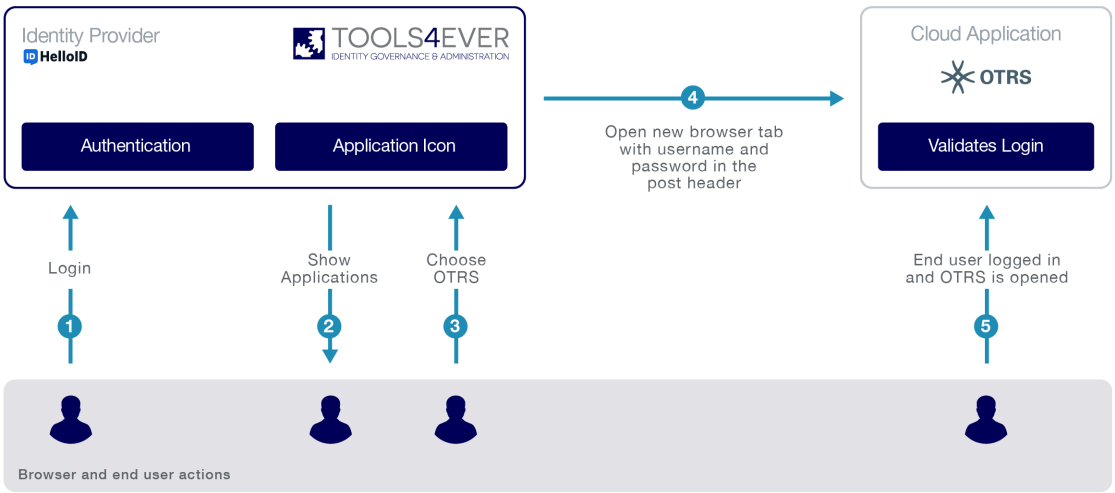


4.3. Le scénario Form POST

Le mécanisme Form POST SSO repose sur l'insertion du nom d'utilisateur et du mot de passe dans l'en-tête de publication HTTP envoyé à l'application Web. Ce mécanisme est également utilisé si un utilisateur accède à l'application via la page de connexion au site Web habituel. La page de connexion affiche les informations d'identification dans l'en-tête (côté client) et l'application (côté serveur) lit ces informations d'identification, les vérifie et authentifie l'utilisateur.

HelloID peut tirer parti de ce mécanisme pour fournir des capacités SSO aux applications qui ne prennent pas en charge les protocoles SSO modernes. L'utilisateur final ressentira le même effet qu'avec SAML : une connexion transparente ne nécessitant aucune interaction utilisateur supplémentaire. HelloID prend en charge à la fois HTTP et HTTPS. Tools4ever recommande fortement ce dernier pour son augmentation substantielle de la sécurité via le cryptage, tandis que le premier échange les informations d'identification en texte clair et non crypté (voir schéma ci-dessous).

Étape 1	L'utilisateur accède au portail HelloID via HTTPS. Chaque client dispose de son propre domaine/URL unique (ma_societe.helloid.com). La première étape est l'authentification de l'utilisateur final.
Étape 2	HelloID affiche le tableau de bord de l'utilisateur contenant toutes les applications auxquelles il peut accéder.
Étape 3	L'utilisateur choisit l'application.
Étape 4	L'utilisateur est redirigé vers l'application avec un formulaire POST contenant les informations d'identification de l'utilisateur.
Étape 5	L'utilisateur est connecté à l'application.



5. LES CONTRÔLES ET LES CERTIFICATIONS HELLOID

Le déploiement d'une solution SSO sécurisée basée sur le cloud commence par les bons principes technologies et partenariaux, comme indiqué dans les chapitres précédents. En outre, nous souhaitons également fournir à nos clients autant de vérifications et de certifications continues que possible. HelloID est indépendamment testé par rapport à des exigences de sécurité claires et conforme aux normes pertinentes. Les vérifications et les certifications sont donc des éléments importants de la politique de sécurité du cloud Tools4ever.

5.1. Scan de Sécurité Deloitte

Chez Tools4ever, nous considérons que les tests proactifs et fréquents de nos solutions de sécurité sont la pierre angulaire de notre succès. Depuis que nous développons des solutions avancées de gestion des identités et des accès, nous avons un grand nombre d'experts en sécurité dans nos propres rangs. Ils ne sont pas seulement actifs dans le développement de nos solutions et produits de sécurité, nous exécutons également un programme interne dans lequel HelloID est testé régulièrement par nos propres experts sur les failles de sécurité potentielles.

Cependant, ce test en interne n'est que notre première ligne de prévention. Nous faisons également tester HelloID en externe deux fois par an par les meilleurs hackers éthiques de Deloitte. En choisissant Deloitte pour cela, nous avons opté pour l'expertise garantie, indépendante et hautement qualifiée du leader du marché de la sécurité de l'information [3].

Ces tests externes nous fournissent une paire d'yeux supplémentaires.

Les tests consistent à attaquer la solution HelloID par un grand nombre de tentatives de pirates informatiques professionnels et éthiques. Ces pirates éthiques ont été formés pour examiner les systèmes informatiques du point de vue d'un cybercriminel expérimenté afin de reconnaître les vulnérabilités que d'autres pourraient ignorer. Par exemple, ils utilisent les directives NCSC ICT-B v2 et les 10 principaux risques de sécurité des applications OWASP de 2013 et 2017.

Les tests couvrent toute la gamme des vulnérabilités potentielles. Par exemple, des rapports système fournissant trop de détails ou la présence de vulnérabilités contenues dans les scripts intersites (XSS). Outre les tests de boîte noire bien connus, les testeurs vont plus loin et exécutent ce que l'on appelle des « tests de boîte grise ». Un « test de boîte grise » recherche les faiblesses de sécurité dans des parties spécifiques de HelloID en utilisant des informations sur la conception et le fonctionnement du logiciel.

Enfin, nous examinons les possibilités pour les utilisateurs autorisés au sein du système. Ont-ils des possibilités « involontaires » qui vont au-delà de ce qui est nécessaire pour leur rôle ? Ceci est essentiel car la fraude et la cybercriminalité ont lieu sont le plus souvent comises par des membres de l'organisation elle-même.

5.2 Certifications

Un élément crucial des services cloud est la conformité aux normes internationales en raison de leur portée mondiale. Cet élément garantit à la fois une intégration correcte avec les systèmes informatiques dans d'autres domaines ainsi que l'adoption des derniers développements en matière de sécurité, de confidentialité et de disponibilité.

Tools4ever a une politique de conformité et de certification active.

OpenID connect

Un exemple récent est notre certification HelloID OpenID. Cette certification confirme la haute qualité de la mise en œuvre d'OpenID Connect dans le cadre de notre solution HelloID Identity-as-a-Service, renforçant encore la confiance de nos clients dans la qualité de nos services.

ISO27001

Nous venons également d'obtenir la certification ISO 2700. Il s'agit d'une norme mondiale de sécurité de l'information. Cette norme spécifie les exigences pour l'établissement, la mise en œuvre, l'exécution, la vérification, la révision, la maintenance et l'amélioration d'un système documenté de gestion de la sécurité de l'information (SMSI) dans le contexte des risques commerciaux généraux pour l'organisation.

En configurant nos solutions Tools4ever conformément à la norme ISO 27001 et en faisant tester et certifier leurs fonctionnements par une partie indépendante, nous avons pu démontrer à nos clients de manière simple, transparente et mondialement reconnue que les solutions Tools4ever sont en règle en matière de sécurité de l'information. Nos clients peuvent faire affaire avec nous en toute confiance. Ceci est très important car nos solutions Tools4ever jouent toujours un rôle central dans leur architecture informatique.

Microsoft Azure

Notre fournisseur Cloud IaaS, Microsoft Azure, maintient le plus grand eventail de conformité du secteur [4], tant en termes d'étendue (nombre total d'offres) que de profondeur (nombre de services destinés aux clients). La conformité couvre les principales normes et certifications applicables à l'échelle mondiale. En outre, Microsoft offre la conformité aux normes et certifications spécifiques à l'industrie, à la région et/ou au pays.

6. CONCLUSION

Dans ce livre blanc, nous avons discuté des aspects de sécurité des capacités d'authentification unique de la solution HelloID. Le document aborde la sécurité de HelloID de deux points de vue différents :

- **Le SSO intègre directement de manière transparente les protections dans le processus de connexion** pour combiner intrinsèquement utilisation intuitive, sécurité et conformité. Réduire les informations d'identification à un seul nom d'utilisateur et mot de passe simplifie l'accès, favorise une culture de sécurité plus disciplinée et prend en charge la conformité aux nouvelles lois sur les données et la confidentialités.
- **La solution SSO elle-même offre une plus grande sécurité grâce à son « point d'accès unique » protégé**. Cela signifie que la sécurité de la solution doit être un élément clé tout au long de son étude, de la mise en œuvre et de son déploiement.

HelloID SSO facilite la convivialité, la sécurité et la conformité

HelloID SSO empêche l'utilisation de plusieurs mots de passe et réduit la notion de « fatigue des mots de passe » et du chaos d'identité. L'utilisation d'un seul ensemble d'informations d'identification favorise la réussite de l'adoption de politiques strictes de changement de mot de passe et de pratiques de stockage de mot de passe sécurisées dans toute l'organisation. Les politiques d'accès configurables de HelloID facilitent considérablement le déploiement du 2FA ou d'autres restrictions d'authentification. Étant donné que l'accès nominatif des utilisateurs aux applications devient beaucoup plus gérable, les organisations peuvent migrer en douceur des comptes partagés vers les comptes personnels. Par conséquent, la conformité de l'organisation aux dernières réglementations en matière de confidentialité et de sécurité des données est à la fois simplifiée et mieux appliquée, tandis que toutes les activités sur la plate-forme peuvent être enregistrées pour des pistes d'inspection, de rapport et d'audit ultérieures.

La Sécurité et l'intégrité de la solution HelloID

Étant donné que le « point d'accès unique » du SSO offre aux utilisateurs un accès complet à l'ensemble des applications et de données affectées à leur rôle ou à leur fonction, la solution requiert une architecture solide et bien entretenue. En utilisant un ensemble clair de principes de conception, de développement et de déploiement de la sécurité, la solution HelloID exploite au maximum les fonctionnalités de sécurité de l'infrastructure en tant que service de Microsoft Azure. La plateforme elle-même prend en charge de nombreuses fonctions de journalisation et de génération de rapports.

Seules les données nécessaires sont stockées dans la base de données chiffrée (RSA-1024 bits) de HelloID. En utilisant le « mappeur d'attributs », le client contrôle parfaitement les données stockées dans la base de données d'HelloID et respecte la politique de confidentialité et de sécurité de l'organisation. Autant que possible, les données sont vérifiées en temps réel dans les systèmes sources connectés.

HelloID peut être intégré à l'Active Directory de l'organisation. Il prend également en charge les principaux fournisseurs d'identité tels que Google, SalesForce, Azure, SAML et LDAP. Alternativement, le répertoire local HelloID est disponible en tant qu'IDP. Pour l'accès aux applications, HelloID prend en charge tous les protocoles SSO existants tels que SAML, HTTP (S) Post, OpenID connect, Oauth, Basic Authentication ou WS-Federation. Pour les applications qui ne prennent en charge aucun protocole SSO, HelloID fournit la connexion unique via une extension de navigateur en mode « Plugin ». De plus, l'authentification à deux facteurs est disponible en tant que deuxième couche de vérification avec des politiques d'accès configurables granulairement et étendues.

La Vérification et les certification HelloID

Enfin, nous souhaitons fournir à nos clients autant de vérifications et de certifications continues que possible. HelloID est indépendamment testé par rapport à des exigences de sécurité claires et conforme aux normes pertinentes. Notre programme complet de certification couvre les tests internes réguliers ainsi que la vérification externe deux fois par an par les meilleurs hackers éthiques de Deloitte, le leader mondial du marché de la sécurité de l'information.

7. A PROPOS DE TOOLS4EVER

Tools4ever propose une large gamme de solutions de sécurité d'entreprise depuis 1999 et est spécialisée dans la gestion des identités et des accès. Au sein du portefeuille de gestion des identités, et en plus du provisionnement des utilisateurs, Tools4ever propose une large sélection de produits de gestion des mots de passe. HelloID est la solution la plus importante de cette gamme. Les autres produits de cette suite sont : la synchronisation des mots de passe entre Active Directory, Mainframe, AS / 400, Unix, Lotus Notes, SAP, etc. (Password Synchronization Manager - PSM) et le Self-service de réinitialisation de mot de passe (Self-Service Password Management - SSRPM).

Des milliers de clients à travers le monde font quotidiennement confiance au bon fonctionnement des logiciels Tools4ever. Pour Tools4ever, la fiabilité et la certification de ses logiciels sont de la plus haute importance. Tools4ever a des partenariats avec les organisations qui s'intègrent à nos logiciels, notamment Microsoft, SAP, Citrix, IBM, Novell et IGEL Technology. Tous les produits Tools4ever concernés sont certifiés par Microsoft et Citrix.

Tools4ever a signé un contrat avec Deloitte Risk Services pour respecter les normes de sécurité les plus élevées. Deloitte Risk Services teste périodiquement HelloID pour détecter d'éventuels problèmes de sécurité.

Tools4ever est aujourd'hui certifié Microsoft Gold Partner, ISO27001, NEN 7510 et OpenID.

8. LES RÉFÉRENCES CITÉES

1	RightScale, „State of the Cloud 2018," 2018.
2	SplashData, [Online]. Available: https://www.teamsid.com/100-worst-passwords-top-50/. [Geopend 15 12 2018].
3	Deloitte, „Deloitte positioned first by Gartner in market share for Security Consulting Services worldwide for sixth consecutive year," 5 october 2018. [Online]. Available: https://www2.deloitte.com/global/en/pages/about-deloitte/articles/deloitte-ranked-1-gartner-in-security-consulting-for-5th-consecutive-year.html.
4	Microsoft, „Microsoft Azure compliance offerings," 29 october 2018. [Online]. Available: https://gallery.technet.microsoft.com/Overview-of-Azure-c1be3942.

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

TOOLS4EVER SOUTH EUROPE

Adresse Calle Ramon Turro 169
08005 Barcelone
Espagne

Tél +34 622 213 732

Informations frsales@tools4ever.com
Support frsupport@tools4ever.com